

# ThreatQuotient



## National Vulnerability Database (NVD) CDF Guide

Version 3.0.1

May 23, 2023

**ThreatQuotient**

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147



ThreatQ Supported

### Support

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://support.threatq.com)

Phone: 703.574.9893

# Contents

- Integration Details..... 5
- Introduction ..... 6
- Installation..... 7
- Configuration ..... 8
- ThreatQ Mapping ..... 10
  - NVD CVE ..... 10
- Average Feed Run..... 16
- Known Issues / Limitations ..... 17
- Change Log..... 18

# Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2023 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

# Support

This integration is designated as **ThreatQ Supported**.

**Support Email:** [support@threatq.com](mailto:support@threatq.com)

**Support Web:** <https://support.threatq.com>

**Support Phone:** 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.



ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

# Integration Details

ThreatQuotient provides the following details for this integration:

|                                  |                   |
|----------------------------------|-------------------|
| Current Integration Version      | 3.0.1             |
| Compatible with ThreatQ Versions | >= 4.27.0         |
| Support Tier                     | ThreatQ Supported |

# Introduction

The National Vulnerability Database (NVD) CVE feed consumes information published by NIST about vulnerabilities. Historic data is provided in a specific package for that year and any new data, updates, or corrections defined from the previous eight days are provided in the "modified" package. Currently, historic records are available for all years between 2002 and present time.

The integration provides the following feed:

- **NVD CVE** - ingests information about vulnerabilities.

The integration ingests the following system objects:

- Indicators
  - Indicator Attributes
- Vulnerabilities
  - Vulnerability Attributes

# Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
  - Drag and drop the file into the dialog box
  - Select **Click to Browse** to locate the integration file on your local machine



ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to [configure and then enable](#) the feed.

# Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** option from the *Category* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

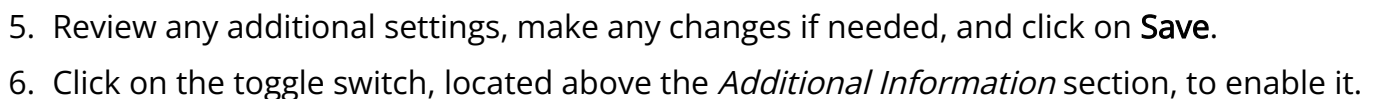
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

| PARAMETER                        | DESCRIPTION                                                                                                                                                                                            |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Save CVE Data as                 | This parameter is required and can be configured to have the feed ingest CVE data such as indicators, vulnerabilities, or both.                                                                        |
| Verify SSL Certificate           | Whether to verify the server's SSL Certificate.                                                                                                                                                        |
| Date used for Filtering the Data | Select which data fields should be used for filtering the data. Options include <b>Publish Date</b> (default) and <b>Modified Date</b> .                                                               |
| CVSSv3 Severity Rating           | Filter the data based on the CVSSv3 Severity Rating. Options include: <ul style="list-style-type: none"><li>◦ All (default)</li><li>◦ Low</li><li>◦ Medium</li><li>◦ High</li><li>◦ Critical</li></ul> |



Enter keyword(s) to be used to filter the results.

Enable this option in the event of using multiple keywords in the parameter above.



# ThreatQ Mapping

## NVD CVE

Scheduled runs ingest CVE data from the "modified" package. Manual runs will request the package for the year specified by the `start_date` parameter. When triggering a manual run, only the year field of the `start_date` is evaluated. If a `start_date` prior to 2002 is selected for a manual feed run, the 2002 package will be requested.



Ingested CVE data can be mapped as CVE Indicators (default configuration), Vulnerabilities, or both.

GET <https://services.nvd.nist.gov/rest/json/cves/2.0>

### Sample Response:

```
{
  "resultsPerPage": 10,
  "startIndex": 0,
  "totalResults": 10,
  "format": "NVD_CVE",
  "version": "2.0",
  "timestamp": "2023-04-07T08:55:08.963",
  "vulnerabilities": [
    {
      "cve": {
        "id": "CVE-2022-41696",
        "sourceIdentifier": "ics-cert@hq.dhs.gov",
        "published": "2023-03-21T23:15:12.167",
        "lastModified": "2023-03-23T16:11:41.357",
        "vulnStatus": "Analyzed",
        "descriptions": [
          {
            "lang": "en",
            "value": "Versions of VISAM VBASE Automation Base prior to 11.7.5 may disclose information if a valid user opens a specially crafted file."
          }
        ],
        "metrics": {
          "cvssMetricV31": [
            {
              "source": "nvd@nist.gov",
              "type": "Primary",
              "cvssData": {
                "version": "3.1",
                "vectorString": "CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N",
                "attackVector": "LOCAL",
                "attackComplexity": "LOW",
                "privilegesRequired": "NONE",
```



ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH                                                         | THREATQ ENTITY                                    | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE                   | EXAMPLES                                                                                                                                                                                  | NOTES                                             |
|------------------------------------------------------------------------|---------------------------------------------------|--------------------------------------|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| .vulnerabilities[].cve.id                                              | Indicator.Value / Vulnerability.Value             | CVE / N/A                            | .vulnerabilities[].cve.published | CVE-2018-6363                                                                                                                                                                             | N/A                                               |
| .vulnerabilities[].cve.descriptions[].value                            | Vulnerability.Description / Indicator.Description | N/A                                  | .vulnerabilities[].cve.published | SQL Injection exists in Task Rabbit Clone 1.0 via the single_blog.php id parameter.                                                                                                       | N/A                                               |
| .vulnerabilities[].cve.lastModified                                    | Vulnerability.Attribute / Indicator.Attribute     | Last Modified                        | .vulnerabilities[].cve.published | 2023-03-24T20:34:11.990                                                                                                                                                                   | Extracted from .vulnerabilities[].cve.id          |
| .vulnerabilities[].cve.id                                              | Vulnerability.Attribute / Indicator.Attribute     | Year                                 | .vulnerabilities[].cve.published | 2018                                                                                                                                                                                      | N/A                                               |
| .vulnerabilities[].cve.references[].url                                | Vulnerability.Attribute / Indicator.Attribute     | Reference URL                        | .vulnerabilities[].cve.published | <a href="https://packetstormsecurity.com/files/146131/Task-Rabbit-Clone-1.0-SQL-Injection.html">https://packetstormsecurity.com/files/146131/Task-Rabbit-Clone-1.0-SQL-Injection.html</a> | N/A                                               |
| .vulnerabilities[].cve.references[].tags[]                             | Vulnerability.Attribute / Indicator.Attribute     | CVE Reference Tag                    | .vulnerabilities[].cve.published | ["Exploit", "Third Party Advisory", "VDB Entry"]                                                                                                                                          | N/A                                               |
| .vulnerabilities[].cve.references[].source                             | Vulnerability.Attribute / Indicator.Attribute     | CVE Reference Source                 | .vulnerabilities[].cve.published | MISC                                                                                                                                                                                      | N/A                                               |
| .vulnerabilities[].cve.configurations[].nodes[].cpeMatch[].criteria    | Vulnerability.Attribute / Indicator.Attribute     | CPE                                  | .vulnerabilities[].cve.published | cpe:2.3:a:taskrabbit_clone_project:taskrabbit_clone:1.0:::*:*                                                                                                                             | N/A                                               |
| .vulnerabilities[].cve.configurations[].nodes[].cpeMatch[].criteria    | Vulnerability.Attribute / Indicator.Attribute     | Affected Vendor                      | .vulnerabilities[].cve.published | taskrabbit_clone_project                                                                                                                                                                  | Parsed in order to extract the needed information |
| .vulnerabilities[].cve.configurations[].nodes[].cpeMatch[].criteria    | Vulnerability.Attribute / Indicator.Attribute     | Affected Product                     | .vulnerabilities[].cve.published | taskrabbit_clone v1.0                                                                                                                                                                     | Parsed in order to extract the needed information |
| .vulnerabilities[].cve.weaknesses[].description[].value                | Vulnerability.Attribute / Indicator.Attribute     | CVE Weakness                         | .vulnerabilities[].cve.published | CWE-89                                                                                                                                                                                    | N/A                                               |
| .vulnerabilities[].cve.metrics.cvssMetricV31.impactScore               | Vulnerability.Attribute / Indicator.Attribute     | CVSSv31 Impact Score                 | .vulnerabilities[].cve.published | 5.9                                                                                                                                                                                       | N/A                                               |
| .vulnerabilities[].cve.metrics.cvssMetricV31.exploitabilityScore       | Vulnerability.Attribute / Indicator.Attribute     | CVSSv31 Exploitability Score         | .vulnerabilities[].cve.published | 2.8                                                                                                                                                                                       | N/A                                               |
| .vulnerabilities[].cve.metrics.cvssMetricV31.cvssData.attackVector     | Vulnerability.Attribute / Indicator.Attribute     | CVSSv31 Attack Vector                | .vulnerabilities[].cve.published | ADJACENT_NETWORK                                                                                                                                                                          | N/A                                               |
| .vulnerabilities[].cve.metrics.cvssMetricV31.cvssData.attackComplexity | Vulnerability.Attribute / Indicator.Attribute     | CVSSv31 Attack Complexity            | .vulnerabilities[].cve.published | LOW                                                                                                                                                                                       | N/A                                               |

| FEED DATA PATH                                                                          | THREATQ ENTITY                                   | THREATQ<br>OBJECT TYPE OR<br>ATTRIBUTE KEY | PUBLISHED DATE                   | EXAMPLES                            | NOTES |
|-----------------------------------------------------------------------------------------|--------------------------------------------------|--------------------------------------------|----------------------------------|-------------------------------------|-------|
| .vulnerabilities[].cve.<br>metrics.cvssMetricV31.<br>cvssData.availabilityImpact        | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv31<br>Availability<br>Impact          | .vulnerabilities[].cve.published | HIGH                                | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV31.<br>cvssData.baseScore                 | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv31 Base<br>Score                      | .vulnerabilities[].cve.published | 6.5                                 | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV31.<br>cvssData.baseSeverity              | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv31 Base<br>Severity                   | .vulnerabilities[].cve.published | MEDIUM                              | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV31.<br>cvssData.confidentiality<br>Impact | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv31<br>Confidentiality<br>Impact       | .vulnerabilities[].cve.published | PARTIAL                             | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV31.<br>cvssData.integrityImpact           | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv31<br>Integrity<br>Impact             | .vulnerabilities[].cve.published | HIGH                                | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV31.<br>cvssData.privilegesRequired        | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv31<br>Privileges<br>Required          | .vulnerabilities[].cve.published | NONE                                | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV31.<br>cvssData.scope                     | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv31<br>Scope                           | .vulnerabilities[].cve.published | UNCHANGED                           | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV31.<br>cvssData.userInteraction           | Vulnerability.attribute /<br>Indicator.Attribute | CVSSv31 User<br>Interaction                | .vulnerabilities[].cve.published | REQUIRED                            | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV31.<br>cvssData.vectorString              | Vulnerability.attribute /<br>Indicator.Attribute | CVSSv31<br>Vector String                   | .vulnerabilities[].cve.published | CVSS:3.0/AV:A/AC:L/PR:N/C:N/I:H/A:H | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV31.<br>cvssData.version                   | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv31<br>Version                         | .vulnerabilities[].cve.published | 3.1                                 | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV30.<br>impactScore                        | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv30<br>Impact Score                    | .vulnerabilities[].cve.published | 5.9                                 | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV30.<br>exploitabilityScore                | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv30<br>Exploitability<br>Score         | .vulnerabilities[].cve.published | 2.8                                 | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV30.<br>cvssData.attackVector              | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv30<br>Attack Vector                   | .vulnerabilities[].cve.published | ADJACENT_NETWORK                    | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV30.<br>cvssData.attackComplexity          | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv30<br>Attack<br>Complexity            | .vulnerabilities[].cve.published | LOW                                 | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV30.<br>cvssData.availabilityImpact        | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv30<br>Availability<br>Impact          | .vulnerabilities[].cve.published | HIGH                                | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV30.<br>cvssData.baseScore                 | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv30 Base<br>Score                      | .vulnerabilities[].cve.published | 6.5                                 | N/A   |

| FEED DATA PATH                                                                          | THREATQ ENTITY                                   | THREATQ<br>OBJECT TYPE OR<br>ATTRIBUTE KEY | PUBLISHED DATE                   | EXAMPLES                            | NOTES |
|-----------------------------------------------------------------------------------------|--------------------------------------------------|--------------------------------------------|----------------------------------|-------------------------------------|-------|
| .vulnerabilities[].cve.<br>metrics.cvssMetricV30.<br>cvssData.baseSeverity              | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv30 Base<br>Severity                   | .vulnerabilities[].cve.published | MEDIUM                              | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV30.<br>cvssData.confidentiality<br>Impact | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv30<br>Confidentiality<br>Impact       | .vulnerabilities[].cve.published | PARTIAL                             | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV30.<br>cvssData.integrityImpact           | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv30<br>Integrity<br>Impact             | .vulnerabilities[].cve.published | HIGH                                | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV30.<br>cvssData.privileges<br>Required    | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv30<br>Privileges<br>Required          | .vulnerabilities[].cve.published | NONE                                | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV30.<br>cvssData.scope                     | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv30<br>Scope                           | .vulnerabilities[].cve.published | UNCHANGED                           | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV30.<br>cvssData.userInteraction           | Vulnerability.attribute /<br>Indicator.Attribute | CVSSv30 User<br>Interaction                | .vulnerabilities[].cve.published | REQUIRED                            | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV30.<br>cvssData.vectorString              | Vulnerability.attribute /<br>Indicator.Attribute | CVSSv30<br>Vector String                   | .vulnerabilities[].cve.published | CVSS:3.0/AV:A/AC:L/PR:N/C:N/I:H/A:H | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV30.<br>cvssData.version                   | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv30<br>Version                         | .vulnerabilities[].cve.published | 3.0                                 | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV2.<br>impactScore                         | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv2<br>Impact Score                     | .vulnerabilities[].cve.published | 5.9                                 | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV2.<br>exploitabilityScore                 | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv2<br>Exploitability<br>Score          | .vulnerabilities[].cve.published | 2.8                                 | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV2.<br>acInsufInfo                         | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv2 AC<br>Insuf Info                    | .vulnerabilities[].cve.published | true                                | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV2.<br>obtainOtherPrivilege                | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv2 Obtain<br>Other<br>Privilege        | .vulnerabilities[].cve.published | false                               | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV2.<br>obtainUserPrivilege                 | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv2 Obtain<br>User Privilege            | .vulnerabilities[].cve.published | false                               | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV2.<br>obtainAllPrivilege                  | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv2 Obtain<br>All Privilege             | .vulnerabilities[].cve.published | false                               | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV2.<br>userInteractionRequired             | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv2 User<br>Interaction<br>Required     | .vulnerabilities[].cve.published | false                               | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV2.<br>baseSeverity                        | Vulnerability.attribute /<br>Indicator.Attribute | CVSSv2 Base<br>Severity                    | .vulnerabilities[].cve.published | HIGH                                | N/A   |

| FEED DATA PATH                                                                         | THREATQ ENTITY                                   | THREATQ<br>OBJECT TYPE OR<br>ATTRIBUTE KEY | PUBLISHED DATE                   | EXAMPLES                                | NOTES |
|----------------------------------------------------------------------------------------|--------------------------------------------------|--------------------------------------------|----------------------------------|-----------------------------------------|-------|
| .vulnerabilities[].cve.<br>metrics.cvssMetricV2.<br>cvssData.accessComplexity          | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv2 Access<br>Complexity                | .vulnerabilities[].cve.published | LOW                                     | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV2.<br>cvssData.availabilityImpact        | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv2<br>Availability<br>Impact           | .vulnerabilities[].cve.published | HIGH                                    | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV2.<br>cvssData.accessVector              | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv2 Access<br>Vector                    | .vulnerabilities[].cve.published | NETWORK                                 | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV2.<br>cvssData.authentication            | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv2<br>Authentication                   | .vulnerabilities[].cve.published | SINGLE                                  | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV2.<br>cvssData.baseScore                 | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv2 Base<br>Score                       | .vulnerabilities[].cve.published | 6.5                                     | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV2.<br>cvssData.confidentiality<br>Impact | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv2<br>Confidentiality<br>Impact        | .vulnerabilities[].cve.published | PARTIAL                                 | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV2.<br>cvssData.integrityImpact           | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv2<br>Integrity<br>Impact              | .vulnerabilities[].cve.published | HIGH                                    | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV2.<br>cvssData.vectorString              | Vulnerability.attribute /<br>Indicator.Attribute | CVSSv2 Vector<br>String                    | .vulnerabilities[].cve.published | CVSS:3.0/AV:A/AC:L/PR:N/C:N/I:H/<br>A:H | N/A   |
| .vulnerabilities[].cve.<br>metrics.cvssMetricV2.<br>cvssData.version                   | Vulnerability.Attribute /<br>Indicator.Attribute | CVSSv2<br>Version                          | .vulnerabilities[].cve.published | 2.0                                     | N/A   |

# Average Feed Run



Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

| METRIC                   | RESULT   |
|--------------------------|----------|
| Run Time                 | 1 minute |
| Indicators               | 142      |
| Indicator Attributes     | 1,999    |
| Vulnerabilities          | 142      |
| Vulnerability Attributes | 1,999    |



---

## Known Issues / Limitations

- The maximum allowable range is 120 consecutive days. If a larger date range is selected, the feed will change the end date to start date plus 120 days.

# Change Log

- **Version 3.0.1**
  - Resolved a bug that appears on the first run.
- **Version 3.0.0**
  - Updated the feed to use the NVD 2.0.0 API
  - Added new configuration options:
    - Date used for Filtering the Data
    - CVSSv3 Severity Rating
    - Filter the results based on Keyword
    - Use Keyword Exact Match
- **Version 2.2.3**
  - Fixed an attribute scoring bug where scoring attributes with a value of 0 were not created.
- **Version 2.2.2**
  - Added description to indicators and vulnerabilities.
- **Version 2.2.1**
  - Documentation updates and more attributes added
- **Version 2.2.0**
  - Update endpoint for NVD's change, `/cve/1.0/nvdcve-1.0-` --> `/cve/1.1/nvdcve-1.1-`
- **Version 2.1.0**
  - Added missing objects attributes
- **Version 2.0.0**
  - Initial release